ABSTRACT

A method and apparatus are disclosed for managing a firewall. The disclosed firewall manager facilitates the generation of a security policy for a particular network environment, and automatically generates the firewall-specific configuration files from the security policy simultaneously for multiple gateways. The security policy is separated from the vendor-specific rule syntax and semantics and from the actual network topology. Thus, the security administrator can focus on designing an appropriate policy without worrying about firewall rule complexity, rule ordering, and other low-level configuration issues. In addition, the administrator can maintain a consistent policy in the presence of intranet topology changes. The disclosed firewall manager utilizes a model definition language (MDL) and an associated parser to produce an entity relationship model. A model compiler translates the entity-relationship model into the appropriate firewall configuration files. The entity-relationship model provides a framework for representing both the firewall-independent security policy, and the network topology. The security policy is expressed in terms of "roles," which are used to define network capabilities of sending and receiving services. A role may be assumed by different hosts or host-groups in the network. A visualization and debugging tool is provided to transform the firewall-specific configuration files into a graphical representation of the current policy on the actual topology, allowing the viability of a chosen policy to be evaluated. A role-group may be closed to prevent the inheritance of roles.